DOWNLOADABLE RESOURCE

25 Cautious AI Prompts for Windows Troubleshooting

Prompts that force evidence, limit assumptions, and slow down destructive repair advice.

Edition: July 2026 **Use:** Personal and business reference

Replace the bracketed text with your own symptoms, command, or output. These prompts are designed to keep AI in a diagnostic role until the relevant drive, file, service, or system state has been confirmed.

Start with evidence

1

Build a fact record first

```
Before suggesting a fix, restate only the facts I have provided. Separate confirmed facts from assumptions and missing information. Ask only the questions that could change the next diagnostic step.
```

2

Classify the risk of every action

```
For every command or setting change you suggest, label it read-only, reversible, or potentially destructive. Explain what it changes, what success looks like, and how to stop safely if the result differs from expectations.
```

3

Do not assume the Windows drive letter

```
Do not assume Windows is on C:. Use the evidence I provide from DiskPart, File Explorer, recovery tools, or command output to identify the correct Windows installation before giving commands that modify a drive.
```

4

Create a one-step diagnostic plan

```
Give me one diagnostic step only. State why this is the next step, what output to capture, and how each likely result changes the diagnosis. Do not give the repair step yet.
```

5 Build an uncertainty list

```
List the possible causes that still fit the symptoms. Rank them by how well they match
the evidence, not by familiarity. Identify one observation that would weaken or
eliminate each cause.
```

Review commands before running them

6 Audit a command

```
Review this Windows command before I run it: [PASTE COMMAND]. Explain each argument,
the files or settings it can affect, whether it requires elevation, and the safest way
to preview or verify the target.
```

7 Require exact targets

```
Do not provide a command containing a drive letter, disk number, partition number,
service name, registry path, or filename until that target has been confirmed from
output I supplied.
```

8 Find the non-destructive version

```
I was advised to run [PASTE COMMAND OR PROCEDURE]. Find the least destructive
diagnostic alternative that can confirm whether the repair is appropriate before
changing the system.
```

9 Check rollback and recovery

```
Before recommending this change, identify the rollback method, any backup or recovery
key needed, and the condition under which I should stop rather than continue.
```

10 Interpret output without guessing

```
Interpret this command output line by line: [PASTE OUTPUT]. Quote the exact lines
supporting each conclusion. State what the output does not establish.
```

Boot, storage, and permissions

11 Map disks and partitions

```
Using only the DiskPart or disk-management output I provide, build a table of each
disk, capacity, partition, filesystem, label, and likely role. Mark any identification
that remains uncertain.
```

12 Verify an EFI repair target

Before giving boot-repair commands, require evidence identifying the Windows partition and EFI System Partition. Explain how to confirm both without formatting, deleting, or recreating anything.

13 Diagnose a boot menu problem

My computer shows multiple Windows boot choices and none works. Build a read-only inspection sequence for BCD entries, Windows installations, EFI files, and disk health. Do not remove boot entries until the correct installation is confirmed.

14 Investigate permissions safely

I changed Windows permissions and now a feature is broken. Help me identify the exact changed path, current owner, inherited permissions, and affected system component before suggesting permission resets.

15 Check storage before cloning

Before cloning a Windows drive, create a preflight review covering source and destination identity, capacity, BitLocker, drive health, backup status, boot mode, partition layout, and post-clone verification.

System files, services, and malware

16 Sequence SFC and DISM correctly

Based on my Windows version and symptoms, explain whether SFC, DISM, or neither is justified. Provide one command at a time and specify what log or result to capture before continuing.

17 Review service changes

I may have disabled Windows services. Use the symptoms and service list I provide to identify likely dependencies. Do not recommend bulk-enabling or disabling services.

18 Separate malware symptoms from system damage

Create a diagnostic plan that distinguishes malware, damaged system files, broken permissions, failing storage, and startup software. Start with observations and read-only checks.

19 Audit a PowerShell repair script

```
Review this PowerShell script for destructive commands, unverified paths, privilege requirements, missing error handling, and rollback gaps. Do not rewrite it until the risks are listed.
```

20 Use official documentation as a constraint

```
For this Windows procedure, compare the proposed steps against current Microsoft documentation. Identify any step that is unsupported, outdated, or being applied outside its documented conditions.
```

Validate the result

21 Define success before repair

```
Before we make changes, define observable success criteria and failure criteria. Include how to verify the original problem is fixed and how to detect a new problem caused by the repair.
```

22 Run a post-change audit

```
After this change, give me a short verification sequence covering the original symptom, Event Viewer or command results where relevant, restart behavior, and any affected data or settings.
```

23 Compare before and after evidence

```
Compare the before-and-after output I provide. Identify only the differences supported by the text. Do not treat a successful command exit as proof that the underlying problem is fixed.
```

24 Know when to stop

```
Based on the symptoms and actions already taken, state the exact conditions under which I should stop troubleshooting and preserve the current state for data recovery or professional repair.
```

25 Final troubleshooting audit

```
Audit this troubleshooting session. List every confirmed fact, every change made, every result observed, unresolved risks, and the next safest step. Identify any earlier conclusion that was based on an assumption rather than evidence.
```

These prompts reduce risk but do not make AI infallible. Preserve important data before repair work and stop when drive failure, encryption, irreplaceable data, or an uncertain disk target is involved.